IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

DONNA CURLING, ET AL., **Plaintiffs,** **v.** **BRAD RAFFENSPERGER, ET AL.,** **Defendants.**	**Civil Action No. 1:17-CV-2989-AT**

DECLARATION OF VINCENT LIU

I, Vincent Liu, declare as follows:

1. I am the CEO and co-founder of the cyber security consulting firm, Bishop Fox, previously known as Stach & Liu. I have been a cyber-security professional since 1999, and my expertise includes network and application security; product security; social engineering; systems and infrastructure security; ethical hacking and penetration testing; cloud security; vulnerability management; red teaming; secure engineering and architecture; security program design; and managing responsible and coordinated disclosure. I have been helping clients locate security vulnerabilities, managing the appropriate disclosure of those vulnerabilities to the appropriate stakeholder, and advising clients on how to remediate and address those vulnerabilities for over fifteen years. I have personal

knowledge of the facts in this declaration and, if called to testify as a witness, I would testify under oath to these facts.

2. I hold a degree in Computer Science and Engineering from the University of Pennsylvania.

3. My career began in 1999 as a security analyst with the National Security Agency (NSA), where I focused on offensive techniques and technologies. The details of my work are classified.

4. After the NSA, I was an ethical hacker[1] for Ernst & Young (E&Y)'s Advanced Security Center, where I performed network and application penetration testing and provided security guidance to many of the largest organizations in the Unites States. As a member of E&Y's Advanced Security Center, my responsibilities included conducting application assessments to identify a broad range of weaknesses within sensitive and critical targets. As an Information Security Specialist, I led the penetration testing team for Honeywell International's global security team, where our mission was to assess and breach the security of Honeywell's IT infrastructure and applications. The team I led performed

[1] The term ethical hacking generally refers to the practice of using hacking tools and techniques to find security vulnerabilities in a target system with the *systems owner's express consent*. The goal of ethical hacking is to find vulnerabilities so those vulnerabilities can be fixed.

penetration testing and source code review against systems, applications, products, and networks across all business units and on multiple continents. I went on to found Bishop Fox in 2006.

5. Bishop Fox has performed security work for 25 of the Fortune 100, 5 of the top 10 global media companies, 10 of the top 20 global retailers, 6 of the top 10 manufacturing firms, and 8 of the top 10 global technology firms. I have personally been involved with many of these clients, specifically in the areas of application security, source code review, application penetration testing, static and dynamic analysis, and secure software development programs.

6. My professional experience includes over 20 years of conducting and managing penetration testing, during which time my team and I have gained significant experience and expertise in compromising and exploiting kiosk-style computer systems (i.e. voting machines, hardened cash safes, ATM machines, bill payment kiosks) similar to those at the center of this litigation. I have often written custom "malware" for the purposes of demonstrating proof-of-concept attacks in systems that were designed to thwart malware. I have and continue to directly advise clients about how to discover, respond to, the threat of malware and chain-of-trust systems.

7. I have presented my research at Microsoft's prestigious invite-only BlueHat conference, where I was one of the first ever to publicly present on security code review techniques. I have also presented at several of the leading security conferences in the world, such as Black Hat and ToorCon. I continue to present and serve as returning faculty for the continuing legal education provider, Practising Law Institute, where I lecture on the topic of cybersecurity to attorneys. I have been cited and interviewed by industry-leading publications (e.g., Dark Reading, CSO Magazine, and The Information) as well as mainstream media (e.g., NPR, USA Today, and Wall Street Journal).

8. I have published short form articles and advice in the top industry news outlets (e.g., Dark Reading and Security Week) and have also contributed to or co-authored seven books published by O'Reilly and McGraw-Hill. Four of these books have been on the topic of application security, and two books in which I have contributed, Sockets, Shellcode, Porting, and Coding and Writing Security Tools and Exploits, both published by Syngress, have been on the topic of "malware" and software security.

9. I have provided further details on my background, experience, and publications in my curriculum vitae attached as **Exhibit 1**.

10. I am not being compensated for work related to this matter and have undertaken to provide my time on a pro bono basis, regardless of the outcome of this litigation, the opinions I express, or any other matter.

11. I have been asked to offer opinions regarding the resilience of security controls implemented to detect instances where Dominion Ballot-marking devices ("BMDs") potentially could be modified by malicious software implants; to offer opinions on the security controls applied to the QR code system used by BMDs to encode voter selections onto a paper ballot; and to offer opinions on the security controls applied to Dominion ImageCast Precinct Scanner and Tabulators ("ICPs"), which have the job of scanning ballot paper QR codes and tabulating the votes encoded therein. I am not undertaking a comprehensive review of the security of Georgia's election system at this time, nor am I addressing every security issue raised in this case at this time. I reserve the right to supplement my opinions as appropriate.

12. I have reviewed the declaration of Mr. Jack Cobb in which he describes the relevant security controls, their intended method of operation, and their fitness for purpose. I offer the following opinions.

13. Malicious software implants on BMDs. It is asserted in Mr. Cobb's Declaration that a BMD has an icon that can be pressed at any time during a vote

to display a SHA-256 hash-based checksum of the BMD's software. The checksum can be visually inspected by election officials to ensure that it matches a known-good expected value.

14. Exactly what software is included in the checksum is not specified, but Mr. Cobb's stated intent is clear: this checksum is intended to present evidence that the BMD is running software that has not been modified by malware.

15. The most obvious flaw with this approach to security is that it ignores that malware can circumvent this check. This approach relies on the equipment to perform integrity checks of itself, which is unreliable and counter to well-accepted cybersecurity principles and practices. A BMD infected with malware could easily report the "correct" SHA-256 checksum and there would be no means to verify whether or not the checksum was valid or a malware deception. In short, the checksum feature provides only what is considered in the cybersecurity community "security theater", not meaningful verifiable integrity validation.

16. QR code security. Once a voter has selected their choices, the BMD prints a paper ballot consisting of two things: the human-readable names of the officials selected by the voter, and a QR code in which the voter's selections are supposed to be encoded. In Mr. Cobb's Declaration he states that "By digitally

signing each QR code the system knows what the content of each QR code should be and will reject any ballot where the digital signatures do not match."

17. It is apparent from this description that BMDs are responsible for and contain all the software code and encryption key material necessary to generate valid QR codes that will be accepted by the ICR tabulation machines.

18. Malware running on a BMD will therefore also have full access to the software code and encryption key material necessary to generate fraudulent QR codes that do not match the voter's selections, but that will nonetheless be accepted as valid by the ICR.

19. It is clear from Mr. Cobb's Declaration that he has conflated QR code *tampering* and QR code *generation*. In my opinion, Mr. Cobb is correct in his declaration that *tampering* with QR codes such that they are invalid might be detected and rejected by the ICR scanner tabulation machines.

20. However, Mr. Cobb failed to address the consequences of malware using the BMD's software against itself to *generate* valid QR codes that do not match a voter's selections. This type of attack is well-known and nothing I saw in the documentation or declarations addresses this highly pertinent gap in Dominion QR code security.

21. The generalized problem of determining if trustworthy code is running on a machine is called "software attestation." Commercial software attestation solutions, such as Intel SGX, employ far more sophisticated techniques to solve this problem than the techniques described in Mr. Cobb's declaration. However, even with these far more advanced techniques, security vulnerabilities were discovered in 2020 that allowed attackers to bypass the Intel SGX attestation solution. This highlights why it is critically important to adopt and enforce rigorous cybersecurity protocols, including reliable, comprehensive assessments of the underlying software and hardware, which should be devised and administered by competent, experienced professionals in the cybersecurity field. This seems especially important with systems as critical as those used to administer elections. Based on my review of the record, I did not see evidence that such protocols are in place for the election system in Georgia and instead identified important mistakes and misunderstandings, such as the reliance on hash values as Mr. Cobb describes.

22. Dr. Halderman's Declarations appear to be technically accurate. The risks, threats models, and outlined attacks are well founded and technically feasible based on available information.

I declare under penalty of the perjury laws of the State of Georgia and the United States that the foregoing is true and correct and that this declaration was executed this 1st day of September, 2020 in San Francisco, California.

By: _____
Vincent Liu

EXHIBIT 1

VINCENT LIU
Managing Partner

As a Partner at Bishop Fox, Vincent Liu is an expert in security strategy, red teaming, and product security; and at Bishop Fox, he oversees firm strategy and client relationships. He has nearly two decades of security experience.

EXPERIENCE

Architected the enterprise application security program for a Fortune 100 manufacturing conglomerate that affected over 2500 developers and more than 30,000 applications supporting four business units in 35 countries. The program involved authoring policy, standards, and guidelines; creation and delivery of custom security training; design of a risk ranking methodology, application assessment program, and threat modeling approach; and deployment of automated assessment tools. Also included were establishing an application inventory, building a remediation program, creating a fix certification process, developing an issue tracking application, and providing security expertise throughout.

Led the only external security consulting team engaged to assist in the development of a secure software development lifecycle for a Fortune 100 microprocessor manufacturer. Activities included developing the software security assurance process, authoring secure coding standards, creating code review and testing checklists, evaluating automated analysis tools, and providing tailored security training.

Headed a team that performed the secure code review of several applications for a Fortune 100 manufacturing conglomerate over the course of 18 months. The assessed applications generated over 1 billion in combined annual revenue and involved the analysis of several million lines of code using a combination of cutting-edge static, dynamic, and manual analysis techniques and methodologies.

TECHNICAL SKILLS AND CERTIFICATIONS

Certified Information Systems Security Professional (CISSP)

CompTIA A+ and Network+

Proficient in Mandarin Chinese

THOUGHT LEADERSHIP

Regularly interviewed by NPR, Al Jazeera, and The Information.

Contributes a column to Dark Reading.

Returning faculty at the Practising Law Institute.

Co-authored seven books (selected): *Hacking Exposed Wireless* *Hacking Exposed Web Applications*.

Presented at Microsoft BlueHat and Black Hat USA among other industry events.

Sits on the advisory boards of Elevate Security, Mod N Labs, and the University of Advancing Technology

Created and delivered on-site, remote, and CBT-based application security, secure programming, and assessment tool training to over 1600 developers in six countries on three continents for a Fortune 100 media conglomerate.

Authored security and regulatory compliance courseware for executives and managers of a Fortune 100 defense contractor. The training material has been and continues to be used to educate hundreds of employees at the managerial level and above.

Led the external security team that provided incident response expertise including malware reverse engineering and traffic analysis for one of the largest and most-publicized security data breach incidents in history.

Oversaw the highly sensitive security review of two applications that at the time were under litigation between two of the largest U.S. credit reporting agencies. The assessment results were used in subsequent negotiations and the final settlement.

Provided security consulting around the development of a Fortune 100 electronics manufacturer's next-generation, customer facing web platform that handles millions of hits per day. Project activities included threat modeling custom mashup frameworks, source code review of the customer portal, evaluation of commercial and open-source security products, developing middleware configuration standards, and authoring security guidelines for Web 2.0 technologies.

Led the team conducting a comprehensive application security review of a health care payment portal for the leading processor of medical claims in the US. The application review included threat modeling, source code review, and penetration testing in observance of HIPAA regulatory requirements.

Advised the leading software-as-a-service provider to assist in preventing phishing attacks against its customers and internal users in addition to securing the overall platform.

EDUCATION

University of Pennsylvania (Philadelphia, PA)

Bachelor of Science in Engineering

Major in Computer Science and Engineering
Minor in Psychology

WRITTEN WORKS BY VINCENT LIU

Books

- **Web Application Security, A Beginners Guide**
  Published Nov. 2014
- **Hacking Exposed: Web Applications, 3rd Edition**
  Published Nov. 2010
- **Hacking Exposed: Wireless, 2nd Edition**
  Published July 2010
- **Hacking Exposed: Wireless, 1st Edition**
  Published March 2007
- **Writing Web Security Tools and Exploits**
  Published March 2006

Contributed Articles

- The Changing Face and Reach of Bug Bounties
  Dark Reading, Published Aug. 2017
- How 'Security Scorecards' Advance Security, Reduce Risk
  Dark Reading, Published Nov. 2016
- Security Leadership & The Art of Decision Making
  Dark Reading, Published Aug. 2016
- How 'Agile' Changed Security At Dun & Bradstreet
  Dark Reading, Published June 2016
- Building A Winning Security Team From The Top Down
  Dark Reading, Published Oct. 2015
- Pen Testing: Making Passion A Priority
  Dark Reading, Published Sept. 2013
- So You Wanna Be A Pen Tester?
  Dark Reading, Published Sept. 2013
- What To Ask Your Penetration Tester
  Dark Reading, Published June 2013
- Beware Of The 'Checklist' Penetration Tester
  Dark Reading, Published May 2013
- Know Your Pen Tester: The Novice
  Dark Reading, Published May 2013
- Better Patching Priority
  Dark Reading, Published March 2013

- Ron Was Wrong, Whit Is Right, And What You Need To Know
  Published March 2012
- Can You Train A Great Penetration Tester?
  Dark Reading, Published Feb. 2012
- Fighting 0days With Fundamentals
  Dark Reading, Published Nov. 2011
- Pro Pen Testing: The Zero-Knowledge Approach
  Dark Reading, Published Oct. 2011
- Secure Development: Using the Right Tools in the Right Place at the Right Time,
  SecurityWeek, Published June 2011
- Silver Bullets only Work in the Movies, Not Security
  SecurityWeek, Published April 2011
- Implementing a Secure Development Lifecycle: The Importance of Executive Support
  SecurityWeek, Published March 2011
- Implementing a Secure Development Lifecycle: Lessons from the Trenches
  SecurityWeek, Published Feb. 2011
- Silly Kiddie, Exploits Are For Free
  SecurityWeek, Published Oct. 2010
- The What And The Why Of Professional Penetration Testing
  Dark Reading, Published Sept. 2010

Blog Posts

- Telling the Security Story: An Interview with Josh Koplik
  Published Nov. 2016
- What Security Leaders Can Learn About Decision-Making
  Published Aug. 2016
- The Power of 'Agile' Security at Dun & Bradstreet
  Published June 2016
- Building a Winning Security Team From the Top Down
  Published Oct. 2015
- A Week in the Life of a Pen Tester
  Published June 2014